Om Desfire

Desfire är en obruten krypteringsstandard för kontaktlösa taggar och kort.

Startpaket

Aras Security erbjuder ett **Desfire Startpaket** som möjliggör för kunden att nyttja Desfire kryptering på kort, utan att bli låst fast till varken producent, distributör eller installatör.

Vid beställning av startpaketet skapar Aras Security en ny Desfire-konfiguration, och levererar därefter samtliga uppgifter till slutkunden. Kunden kan sen själv fördela ut behörigheter (nycklar) till intern eller extern kortproduktion, och till konfiguration av kortläsare som blir låsta till kundens kort.

Om kunden önskar att deras installatör eller systemleverantör äger nycklarna kan Aras Security leverera dessa efter önskemål.

Startpaket – Detta ingår

- Skapande av unik konfigurationsnyckel.
  Detta innebär att kortläsaren inte kan konfigureras utan denna nyckel, dvs kortläsaren är skyddad mot manipulation.
- Skapandet av unika Desfire-nycklar.
  Dessa nycklar skyddar mot kopiering av korten.
  Alternativt skapas diversifierade nycklar, om kortläsaren stödjer detta.
- Skapandet av ett artikelnummer för att underlätta beställning av färdigkonfigurerade kortläsare. Artikeln blir endast tillgänglig för behöriga kunder (installatörer) till Aras Security.
- 2 konfigurationskort för att möjliggöra ändring av adress på kortläsaren från 0->1 samt från 1->0 (in- och utläsare).

Engångskostnad: 15000kr*

* Pris för startpaket rabatteras vid samtidigt köp av kortläsare, se mer på vår hemsida.

Tillval

- USB-läsare som konfigureras för att läsa kortnummert från den låsta filen på kundens taggar/kort.
  Engångskostnad: 5000kr

- Konfiguration som även tillåter kortläsarna att läsa osäkra kort, t.ex. Mifare Classic UID (Unique identity)
  Notera att detta förutsätter att kortläsaren kan hantera läsning av båda format samtidigt. Detta rekommenderas ej, då det komprimerar säkerheten på de kortläsare som endast läser öppet UID.
  Engångskostnad: 1000kr

- Addera ytterligare en kortläsarmodell med samma konfiguration. S
  Engångskostnad: 9500kr

Kortproduktion

Aras Security erbjuder färdigprogrammerade kort eller taggar till Desfire-konfigurationen.
Installatören kan därmed köpa kort och taggar samt kortläsare som är färdigprogrammerade i kundens format.

Aras Security säljer även programvara och kortprinter om kunden själv önskar producerar korten.

Tekniska specifikationer om formatet

Aras Security skapar 3 låsta filer som innehåller ett kortnummer.

Fil 1 och 2 används av kundens kortläsare.

Fil 3 kan användas om ett annat system vill läsa ut kortnumret från en fil.

Alla filerna är säkra och skyddade.

Fil 1

Denna fil använder *diversified keys*, vilket betyder att filen är skyddad med en unik nyckel för varje kort. Detta görs genom att kortnumret kombineras med en säker nyckel. Denna nyckel är känd för kortläsaren, som därmed kan läsa ut kortnumret.

Om ett kort blir komprimerat och nyckeln blir känd, kommer endast detta kort vara komprimerat då inget annat kort har samma nyckel. Endast kundens kortläsare kommer kunna läsa ut kortnumret från denna fil.

Fil 2

Denna fil är skyddad av nycklar som endast kundens kortläsare känner till. Kortläsarna kommer endast leta efter kortnumret i denna fil, med kundens nycklar. Fil 2 används på kortläsare som inte stödjer *diversified keys* (läs fil 1).

Fil 3

Fil 3 är samma som fil 2, men kundens kortläsare använder inte denna fil alls. Denna fil är skapad för att underlätta användandet av korten i andra system som vill läsa ut kortnumret från en säker fil på Desfire-kortet.

Tekniskt sätt kan även fil 1 eller fil 2 användas för detta, men det förutsätter att kunden ger tillgång till säkerhetsnycklarna för filerna som kortläsarna användas, vilket komprimerar säkerheten i anläggningen. Tredjepartsystemet som ska läsa kortnummer i fil 3 kan endast skapa kort som kan läsas i deras system, inte i kundens passersystem.

Kombinera Desfire-kort med osäkra kortläsare

Om kunden önskar använda samma kort för att läsa på osäkra kortläsare används kortets UID som kortnummer. Detta betyder att konfigurationen tar kortets UID och lägger detta i samtliga filer.

Denna metod gör att korten är öppna för läsas av ett annat Desfire-krypterat system, samt system som endast kan läsa ut UID från kortet. Detta komprimerar inte säkerheten på de kortläsare som har kortnumret i filer som är skyddade med krypteringsnycklar, då dessa förutsätter krypteringsnycklar för att läsa ut kortnumret.

Detta medför ytterligare kostnader, kontakta Aras Security för mer information.